Chapter 16
Legal aspects of operating IoT applications in the Fog

G. Gultekin Varkonyi, Sz. Varadi and A. Kertesz

16.1 Introduction

As a growing number of communicating devices join the Internet, we will soon face a foggy and cloudy world of interconnected smart devices. Cloud systems [1] already started to dominate the Internet, with the appearance of things of the Internet of Things (IoT) area [2] IoT Cloud systems are formed that still needs a significant amount of research. IoT is a rapidly emerging concept where sensors, actuators and smart devices are often connected to and managed by cloud systems. IoT environments may generate a huge amount of data to be processed in the Cloud. To reduce service latency and to improve service quality, the paradigm of Fog Computing [5] has been introduced, where the data can be kept and processed closed to the user.

The European Commission is currently in the last phase of reforming the European data protection rules, where the main objectives are: to modernize the legal system of the European Union (EU) for the protection of personal data to respond to the use of new technologies: to strengthen users' influence on their personal data and to reduce administrative formalities, and to improve the clarity and coherence of the EU rules for personal data protection. To achieve these goals, the Commission created a new legislative proposal, called General Data Protection Regulation (GDPR) [3], a regulation that sets out a general EU framework for data protection to replace the currently effective Data Protection Directive (DPD) [4]. In IoT Cloud systems, personal data is

increasingly being transferred possibly across borders and stored on servers in multiple countries both within and outside the EU. The globalized nature of dataflow calls for strengthening the individuals' data-protection rights internationally. This requires strong principles for protecting individuals' data, aimed at easing the flow of personal data across borders while still ensuring a high and consistent level of protection without loopholes or unnecessary complexity. In these legal documents the Commission aims to introduce a single set of rules on data protection.

The Regulation, unlikely to the former Directive, exceeds its jurisdiction outside of the EU and abides by its rules of all the actors that offer services to the EU citizens, regardless of their residence. The GDPR also introduces some of the new rights that were a natural result of the technological developments, such as data protection by design and right to be forgotten. However, the technical structure and complexity of the IoT and the Fog make it hard to be implemented and as a result, make it hard to comply with the law. For this reason, the importance of "thinking the data protection rights of the people from the early phase of the system development", called as Data Protection by Design, is also placed in the Regulation [3]. Data Protection by Design aims to reduce possible privacy harms that Fog applications may cause by combining it with the Data Protection Impact Assessment and the Data Protection Enhancing Technologies.

In this chapter we classify Fog/Edge/IoT applications, analyze the latest restrictions introduced by the GDPR, and discuss how these legal constraints affect the design and operation of IoT applications in Fog and Cloud environments.

16.2 Related work

Security concerns for IoT have already been investigated by Escribano [6], who presented the first opinion [7] of the Article 29 Data Protection Working Party (WP29) in this regard. They stated in this report that it is crucial to identify and realize which stakeholder is responsible for data protection. WP29 named the following challenges concerning privacy and data protection: lack of user control, low quality of user consent, secondary uses of data, intrusive user profiling, limitations for anonymous service usage, and communication- and infrastructure-related security risks.

Yi et al. [8] further extended these concerns with respect to Fog Computing. They presented a survey, in which they argue that secure and private data computation methods are needed, and privacy need to be addressed in three dimensions: data, usage and location privacy. As Fog nodes can be geographically distributed it is even more difficult to track and monitor data and its location in real time. Furthermore, when distributed and processed data is merged, the integrity of the data should be guaranteed. Fog node can also track end user devices to support mobility (location awareness) that may be a game changing factor for location-based services and applications. This puts location privacy of the user at risk, and therefore appropriate location preserving privacy mechanisms must be employed. From security perspective, man-in-the-middle attack has a high potential to become a typical attack in Fog Computing. In this attack, nodes serving as Fog devices may be compromised or replaced by fake ones. Traditional anomaly detection methods can hardly expose man-in-the-middle attack without noticeable features of this attack collected from the Fog [9].

Mukherjee et al. further detailed these challenges in [10]. They envisaged a three-tier fog architecture, where communication is performed through three interfaces: fog-cloud, fog-fog and fog-things. They stated that secure communication is a key issue,

and privacy-preserving data management schemes are needed. They mentioned, but did not detail legislation challenges, which is the aim of this chapter.

16.3 Classification of Fog/Edge/IoT applications

In the past decade we experienced an evolution in Cloud Computing: the first clouds appeared in the form of a single virtualized datacenter, then broadened into a larger system of interconnected, multiple datacenters. As the next step, cloud bursting techniques were developed to share resources of different clouds, then cloud federations [11] were realized by interoperating formerly separate cloud systems. There were various reasons to optimize resource management in such federations: to serve more users simultaneously, to increase quality of service, to gain higher profit from resource renting, or to reduce energy consumption or CO2 emissions. Once these optimization issues were addressed and mostly solved, further research directions started to use clouds to support newly emerging domains, such as the Internet of Things. In the case of IoT systems, data management operations are better placed close to their origins, thus close to the users, which resulted in better exploiting the edge devices of the network.

Finally, as the latest step of this evolution the group of such edge nodes formed the fog. Dastjerdi and Buyya defined fog computing as a distributed paradigm [5], where cloud storage and computational services are performed at the network edge. This new paradigm enables the execution of data processing and analytics application in a distributed way, possibly utilizing both cloud and near-by resources. The main goal is to achieve low latency, but it also brings novel challenges in real-time analytics, stream processing, power consumption and security.

Concerning IoT application areas Want et al. [12] set up three categories to classify them: (i) Composable systems, built from a variety of nearby interconnected

things; (ii) Smart cities, utilities of modern cities such as a traffic-light system capable of sensing the location and density of cars in the area; (iii) Resource conservation applications, used for monitoring and optimization of resources such as electricity and water. Atzori et al. [13] proposed a survey and identified five domains: transportation and logistics, healthcare, smart environments (home, office, plant), personal and social, finally futuristic domains. In this chapter we do not aim to classify all application fields, but to define certain architectures that fit most application cases involving cloud, IoT and fog utilization, to enable further investigations concerning security and privacy.

From this discussion we can see that the collection, aggregation and processing of user data can be done is various ways. Figure 16.1. presents an architecture, where certain data flows can be examined.

In the next section we summarize legislation affecting these tasks, and later we give guidelines on how to comply with such regulations in the identified cases.

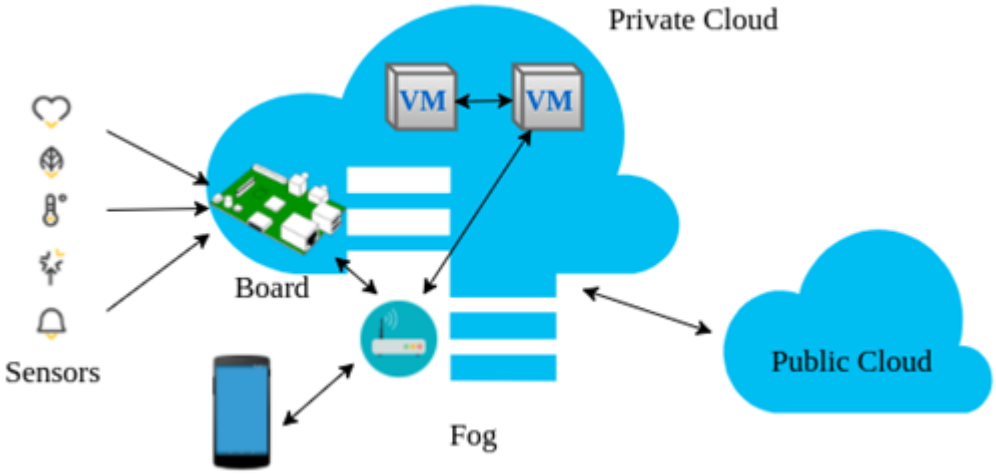

Figure 16.1. Data management in fog environments.

16.4 Restrictions of the GDPR affecting Cloud, Fog and IoT applications

The European Union is currently in the last phase of reforming the European data protection rules, where the main objectives are: to modernize the EU legal system for the protection of personal data to respond to the use of new technologies; to strengthen users' influence on their personal data and to reduce administrative formalities; and to improve the clarity and coherence of the EU rules for personal data protection. To achieve these goals, the Commission created a new legislative proposal, called General Data Protection Regulation a Regulation (GDPR) [3] that sets out a general EU framework for data protection to replace the currently effective DPD. Personal data is increasingly being transferred across borders and stored on servers in multiple countries both within and outside the EU. The globalized nature of data-flows calls for strengthening the individuals' data protection rights internationally. This requires strong principles for protecting individuals' data, aimed at easing the flow of personal data across borders while still ensuring a high and consistent level of protection without loopholes or unnecessary complexity. According to the Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), the protection of natural persons in relation to the processing of personal data is a fundamental right. But the GDPR states that this is not an absolute right, it must be considered in relation to its function in society and be balanced against other fundamental rights.

Because of new challenges for the protection of personal data like rapid technological developments and globalization, the scale of the collection and sharing of personal data increased significantly. Both private companies and public authorities can use of personal data on an unprecedented scale in order to pursue their activities

and beside that, natural persons increasingly make personal information available publicly and globally. Therefore, the European Union makes an emphasis on development of digital economy inside of the internal market with the free flow of the personal data without any barriers, but in frame of a coherent and strong data protection. The protection of individuals should be technologically neutral so it does not depend on the techniques used; otherwise this would create a serious risk of circumvention.

16.4.1 Definitions and terms in the GDPR

The new data protection framework of the EU called GDPR [3] contains new rules and tools to fulfil these goals. It will enter into force on May 2018 and from that time the level of protection of the rights and freedoms of individuals with regard to the processing of such data would be equivalent in all Member States. In the following we gather the newly introduced, relevant terms and rules of the GDPR, and later we analyze them with the operational aspects of Fog computing.

Personal data. It could be any information relating to an identified or identifiable natural person such as name, identification number, location data and online identifier or to one or more indicators specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data subject. A natural person, who is identified or identifiable. The identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to his or her personal data.

Controller. A natural or legal person, public authority, agency or other body can play this role. This new element under the GDPR is that the controller determines also the conditions of the processing of personal data.

Processor. It is also an important actor, who is also a natural or legal person, public authority, agency or other body could be, which processes personal data on behalf of the controller.

Pseudonymization. It is a new term, which means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Limitation. What has a great importance among the principles relating to personal data processing is the limitation. Purpose of the collection, the quality of the data and the duration of the storage are all limited based on their necessity. New elements are in particular the transparency principle, the clarification of the data minimization principle and the establishment of a comprehensive responsibility and liability of the controller.

Consent. In order for personal data processing to be lawful, it has to be on the basis of the consent of the data subject for one or more specific purposes. The processing should be necessary for the performance of a contract in which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. More specifically:

- processing is necessary for compliance with a legal obligation of the controller;
- processing is necessary in order to protect the vital interests of the data subject;

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Regarding the conditions for consent, the data subject shall have the right to withdraw his or her consent at any time. In this case, the lawfulness of the former processing should not be affected by the withdrawal of consent. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller. In order to have one single and consistent definition, the GDPR contains that “consent” means any freely given, specific, informed and unambiguous agreement of the data subject to the processing of personal data relating to him or her. It could be given either by a statement or by a clear affirmative action. So it should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes. Therefore, silence or inactivity should not create the consent. Consent has to cover all processing activities carried out for the same purpose. The processing of the personal data of a child shall be lawful where the child is at least 16 years old and after his or her consent was given. Where the child is below the age of 16 years, such processing shall be lawful only if the consent was given or authorized by the holder of parental responsibility over the child.

Right to be forgotten. The GDPR further elaborates and specifies the data subject's right of erasure and provides the conditions of the right to be forgotten, when the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. Another case is when the data subject withdraws consent on which the processing is based, or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data. This means the obligation of the controller which has made the personal data public to inform third parties to erase any links to, or copy or replication of that personal data. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorized the publication by the third party. The controller shall carry out the erasure without delay, but there are some exceptions when the retention of the personal data is necessary e.g. for exercising the right of freedom of expression or for reasons of public interest in the area of public health; for historical, statistical and scientific research purposes etc. Where the erasure is carried out, the controller shall not otherwise process such personal data.

This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially from the Internet.

Data portability. The GDPR introduces the data subject's right to data portability, i.e. to transfer data from one electronic processing system to, such as a social network, into another, without being prevented from doing so by the controller. As a precondition and in order to improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format. This option could apply where the data subject provided the

data to the automated processing system, based on their consent or in the performance of a contract.

16.4.2 Obligations defined by the GDPR

The data subject has the right to object a measure based on profiling solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyze or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior.

Obligations of the controller. The GDPR introduces the obligation on controllers to provide transparent, easily accessible and understandable information, inspired in particular by the Madrid Resolution on international standards on the protection of personal data and privacy (Madrid Resolution, 2009). Another obligation of the controller is to provide procedures and mechanism for exercising the data subject's rights, including means for electronic requests, requiring response to the data subject's request within a defined deadline (at the latest within one month of receipt of the request), and the motivation of refusals.

There is information obligation of the controller towards the data subject, too. The controller shall provide all the information about:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
b) the contact details of the data protection officer, where applicable;
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is necessary for the purposes of the legitimate interests, about the legitimate interests themselves pursued by the controller or by a third party;
e) the recipients or categories of recipients of the personal data, if any;
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission.

There are some additional pieces of information, which shall be given by the controller like the storage period; the right to withdraw the consent any time; access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; the right to lodge a complaint with a supervisory authority and the existence of automated decision-making including profiling as well as the significance and the envisaged consequences of such processing for the data subject. The data subject could request a confirmation from the controller at any time, whether or not personal data relating to the data subject are being processed.

Data protection by design and by default. To ensure privacy and data security, the GDPR introduces a new term called data protection by design (or privacy by design in the draft proposal of the GDPR). It means that the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures considering the state of the art and the cost of implementation, in such a way that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Such measures should include minimizing the processing of personal data, and applying pseudonymization on the personal data as soon

as possible. The appropriate system should also enable the data subject to monitor the data processing, and the controller to create and improve security features. This principle and the named measures are particularly important in designing Fog environments. These measures shall be steps to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing in particular any unauthorized disclosure, dissemination or access, or alteration of personal data. We further detail these issues in the next section.

Regarding to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

Articles 26 and 27 address some of the issues raised by Cloud Computing, more specifically from Cloud Federations. While these provisions do not indicate whether outsourcers are joint data controllers, they acknowledge the fact that there may be more than one data controller. The provision of the GDPR clarifies the responsibilities of joint controllers as regards their internal relationship and towards the data subject. Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under the GDPR, by means of an arrangement between them.

Those controllers or processors, who are not established in the Union, have an obligation to designate a representative in the EU in a written form, where the GDPR applies to their processing activities. The exceptions are when the data processing is

occasional and includes not special categories of data or when the controller is a public authority or body. The representative should act on behalf of the controller or processor and may be addressed by any supervisory authority.

The main establishment of a controller in the EU should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. Only the presence and use of technical means and technologies for processing personal data do not constitute such main establishment themselves and are therefore no determining criteria for a main establishment. The main establishment of a controller or a processor should be the place of its central administration in the EU and implies the effective and real exercise of activity through stable arrangements according to the GDPR.

Obligations of the Processor. The GDPR also clarifies the position and obligation of processors adding new elements, including that a processor who processes data beyond the controller's instructions is to be considered as a joint controller. The Regulation requires that the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet ensure the protection of the rights of the data subject. The processor shall not apply another processor without prior specific or general written authorization of the controller.

The carrying out of processing by a processor shall be governed by a written contract or other legal act including in electronic form, binding the processor to the controller and stipulating in particular that the processor shall:

- act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

- employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
- take all required measures;
- enlist another processor only with the prior permission of the controller;
- insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organizational requirements for the fulfilment of the controller's obligation;
- assist the controller in ensuring compliance with the obligations;
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless EU or Member State law requires storage of the personal data;
- make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in the GDPR.

This contract or legal act should contain in whole or in part, on standard contractual clauses, including when they are part of a certification granted to the controller or processor in accordance with the provisions of the GDPR regarding the certification. The European Commission could lay down additional standard contractual clauses.

The controller and the processor shall document in writing the controller's instructions and the processor's obligations. The processor shall be considered to be a

controller in respect of that processing and shall be subject to the rules on joint controllers, if a processor processes personal data other than as instructed by the controller.

GDPR introduces the obligation for controllers and processors to maintain a record of processing operations under their responsibility in written and in electronic form, instead of a general notification to the supervisory authority required by the former Directive of the EU. It shall contain some relevant information such as the purpose of the data processing, the name and contact details of the controller or the processor and description of the categories of data subjects and of the categories of personal data, etc.

The GDPR introduces an obligation to notify personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC. Moreover, the former DPD provided for a general obligation to notify processing of personal data to the supervisory authorities, which notification could create administrative and financial burdens. According to the Commission, this general obligation should be replaced by effective procedures. Therefore, the new Regulation introduces a new element, namely the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations, which could present specific and high risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. According to the GDPR the following processing operations in particular present specific risks:

- “a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including pro-

filing, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
- a systematic monitoring of a publicly accessible area on a large scale."

About those processing operations which require data protection impact assessment, a public a list should be created by the supervisory authority. The impact assessment shall contain at least:

- a detailed description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

This provision should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

The GDPR contains that the controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, building on the concept of prior checking in Article 20 of DPD.

The new Regulation, based on Article 18(2) of DPD, introduces also the function of a mandatory data protection officer, who should be designated when the processing carried out for the public sector or for large enterprises, or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring or consist of processing on a large scale of special categories of data. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

Article 40 concerns codes of conduct, building on the concept of Article 27(1) of DPD, clarifying the content of the codes and the procedures. The Member States, the Commission, the supervisory authorities and the Board shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The monitoring of compliance with a code of conduct may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

16.4.3 Data transfers outside the EU

Data transfer to third countries. The Chapter V of the GDPR contains the rules for transfers of personal data to third countries or international organizations. According to the new provisions, transfer could be carried out only when an adequate level of

protection is ensured by the third country, or a territory or a processing sector within that third country, or international organization in question. The new provision now confirms explicitly that the European Commission is in the position to decide whether this adequate level of protection is provided by a territory or a processing sector within a third country.

The criteria which shall be taken into account for the Commission's assessment of an adequate or not adequate level of protection include expressly the rule of law, respect for human rights and fundamental freedoms, relevant legislation and independent supervision. It is also important that the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Where the Commission decides that an adequate level of protection is ensured a so called implementing act shall create for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organization. The Commission has the duty to monitor these developments.

A list of those third countries, territories and processing sectors within a third country and international organizations, where it has decided that an adequate level of protection is or is not ensured, should be published by the Commission in the Official Journal of the European Union.

When no such an adequacy decision has been adopted by the Commission, the GDPR requires for transfers to third countries, to provide appropriate safeguards, in particular:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;
- standard data protection clauses adopted by the Commission or by a supervisory authority;
- an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

The GDPR explicitly provides for international co-operation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries like mutual assistance.

The draft version of the GDPR contained provisions for that case, if the Commission decided the adequate level was not ensured in a third country or a territory etc. third country or a territory within that third country, or the international organization, any transfer of personal data to that place in question should be prohibited. In this case, the Commission should enter into consultations with this third country or international organization to remedying the situation resulting from this inadequacy decision. Such statement of the Commission is missing from the final version of the GDPR.

In the absence of an adequacy decision or of appropriate safeguards, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and other natural or legal person;
d) the transfer is necessary for important reasons of public interest;
e) the transfer is necessary for the establishment, exercise or defense of legal claims;
f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent

that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information to the data subject of the transfer and on the compelling legitimate interests pursued.

Remedies, liability, sanctions. The Regulation contains provisions for remedies, liability and sanctions. The new Regulation concerns the right to a judicial remedy against a controller or processor, providing a choice to go to court in the Member State where the defendant is established or where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

If material or non-material damage was caused by an infringement of the GDPR, the controller or processor shall provide compensation for the damage suffered. One of the possible penalties could be administrative fines; besides that, other penalties should be laid down by the Member States.

16.4.4 Summary

As a summary, due to the legal nature of a regulation under EU law, the GDPR will establish a single rule that applies directly and uniformly. EU regulations are the most direct form of EU law. A regulation is directly binding upon the Member States and is directly applicable within the Member States. As soon as a regulation entered into force, it automatically becomes the part of the national legal system of each Member State and it is not allowed to create a new or different legislative text by each Member State. Contrarily, EU directives are flexible tools of the EU legislation; they are used to harmonize the different national laws in-line with each other. Directives prescribe

only an end result that must be achieved by every Member State; the form and methods of implementing the principles included in a directive are a matter for each Member State to decide for itself. Each Member State must implement the directive into its legal system, but can do so in its own words. A directive only takes effect through national legislation that implements the measures.

We revealed in a former work on Cloud federations [14] that according to the Article 4 of the current DPD, the location of the data controller's establishment determined the national law applicable, which could be variable as we have seen in specific cloud use cases. However, the GDPR with its unified rules after entering into force must be applied in every Member State in the same way, so there would be and could be not discrepancy among them. Moreover, where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the EU, such as in a Member State's diplomatic mission or consular post. (Preamble (22) of GDPR).

In the next section we further detail the data protection by design principle, and discuss its implementation needs and its possible causes.

16.5 Data protection by design principles

The Privacy by Design (PbD) concept was comprehensively explained in the 90’s by Ann Cavoukian who is the former Information and Privacy Commissioner for the Canadian province of Ontario. Her philosophy received high level of attention not only from the privacy scholars but by the legislators, too. Such that, Article 25 was placed into the GDPR which legally binds the data controllers to take several technical and organizational measures to comply with the related law. The GDPR uses the title “Data Protection by Design (DPbD)” as it focuses only on the data protection,

however, there is no difference between the two terms both in the legal and practical meaning. We will also follow the GDPR's notion in this chapter.

Cavoukian [15] uses Fair Information Practices Principle as a basis for the DPbD principles. These principles could, as could be found in the GDPR too, be counted as follow: data minimization; data retention and data usage limit (purpose specification); individual consent; notice responsibility (transparency); stored data security; right to access to own personal data; and accountability. Her solution for the serious privacy risks in the highly growing technological environment foresees to develop such systems that are not interrupted by the privacy rules, but to make these rules an integral part of the "organizational priorities, project objectives, design processes, and planning operations". In order to do that, the DPbD philosophy should be adopted from the beginning of the system design [16], and should follow the system's life-cycle until it becomes useless. Today, system design does not only mean the technical part of the system creation, such as code developing. Many different technological solutions offered by the IT companies consider organizational aspects to the legal compliances, during the system design. For this reason, it is possible to say that the concept of the DPbD is in relation with both legal and technical, as well as organizational aspects. It is legal, because the legal developments trigger the adoption of the DPbD. It is organizational, because it means self-assessment, self-regulation and self-reaction to reach the privacy-friendly technologies. It is technical, because as a result of the legal requirements and the organizational planning, tangible steps are required towards privacy-friendly systems. This step generally requires technical solutions to involve with the system, which are called as the Privacy Enhancing Technologies (PETs). Through PETs, the DPbD becomes visible by the end-user. Altogether, DPbD means to draw the map of the personal data collection, usage, transmission, access,

storage, shortly any processing activity, as well as the business models behind the personal data, and taking the necessary technical safeguards to ensure security of the data in a certain system that reduces users' data protection concerns.

16.5.1 Reasons for adopting data protection principles

Before we go into the details, one may ask the reason why to adopt DPbD principles. Firstly, if data protection is a fundamental right and if it should be taken into account from the beginning of the system design, then, the DPbD concept is the one that can create the "data protection first" [17] culture. This culture leads the company to gain user trust. Whenever the Internet users share personal data online, they trust the promises of the service providers on data collection, usage, storage and safety. Only with user trust the Internet economy can grow [18] because more DPbD friendly systems will be used by more people [19]. This might be one of the reason why Apple grows, because "at Apple, our trust means everything to them" and "that's why they respect our privacy and protect it with strong encryption…" [20] and other techniques.

Secondly, the organizations will fully comply with the legal obligations so they will not be faced with huge amount of fines and will not lose money. Similarly, as much as possible to foresee the risks, the organizations will spend fewer money to fix them than after launching the product [21]. More sanctions lead to more reputation loss, either [22]. In addition, the organizations will create data protection culture [23] automatically in the company. Moreover, as the technology changes very fast and develop so quickly, it is not easy to control the privacy concerns during the system usage. It is necessary to foresee such dangers from the beginning of the basic system design and simply do the right thing. Additionally, the whole philosophy can contribute

to the global data protection which is missing because of different data protection understanding and implementations.

Finally, DPbD helps reducing the world data protection asymmetry, power games and political conflicts, and promotes free flow of information, national security and democracy. It is a philosophy to be embraced against surveillance, misuses and illegal uses. Thanks to the globalization and to the Internet, where there is a product like Facebook, with the help of the data protection leading countries' legal pressure now everybody benefits from the same data protection shield in the world [16].

16.5.2 Privacy protection in the GDPR

Now, taking a closer look at the principles of the DPbD could give more comprehensive understanding of what exactly is indicated by the DPbD as a privacy protection. Regardless of its orders, the first principle appears to be the logic of the whole DPbD understanding, which points out the current problem of being unable to fix the data leakage once it happens. Interconnected online networks do not seem helpful to fix unwanted data disclosures due to the fact that it is not possible to find out all the possible connections of an online personal data. Once the data is online, it is almost impossible to destroy it in the online world. Proactive and Preventative approach to personal data protection lowers the risk of such disclosures in a way that adopting even higher standards than the already known ones, creating privacy network between the users and partners, and realizing the privacy-weak points of the systems. From the system point of view, this requires to embed privacy into the system's architecture. One of the way to find out what kind of privacy tools exactly to be embedded into the systems could be found through the Privacy Impact Assessments. Article 35 of the GDPR brings Data Protection Impact Assessment (DPIA) responsibility to the data

controllers when data processing is "likely to result in a high risk to the rights and freedoms of natural persons". The fact is that, any system deals with personal data carries some level of risk. In order to define the level of risk and take necessary steps, DPIA is the first attempt on the way to PDbD and success of the PDbD depends highly on a successful DPIA [23].

DPIA is a systematic way of assessing the risks that will lead the businesses together with their stakeholders and employees to know what and how to handle the risks related to data protection in a certain system(s). Target of the DPIA is to help the organizations to create complete picture of the personal data collection, storage, usage, transfer, and finally managing the risks appearing in these processes. The relationship between the DPbD and the DPIA is two-folded; they feed each other, because in the end, data protection measures and the techniques will be "pro-actively" built into the systems. The result of the assessment helps decision-makers to have a plan on how to strengthen the data security which directs them to decide on what PETs to implement.

PETs are perhaps described best in the EU literature especially from the data protection point of view:

"It is a system of Information and Communication Technologies measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system" [24]. The PETs are not newly referred in the EU data protection literature, however, the GDPR was widened and explained (Recital 78) them. They are the technical tools that help organizations to reduce the risks appeared through DPIA. These tools are, in general, encryption, email privacy tools, anonymization and pseudonymization tools, authentication tools, cookie cutters,

The Platform for Privacy Preferences, etc. The list is non-exhausted, due to the fact that privacy protection and especially data protection technology will grow ever faster after May 2018, when the GDPR enters into force.

16.5.3 Data protection by default

Secured systems combining with the data processing principles consists the Privacy by Default or, with the GDPR words, Data Protection by Default (DPbD) concept. Basically, DPbD is related to the data minimization principle and orders to the data controller to collect as minimum as possible personal data during the services. This does not mean to interrupt the system functionality and does not refrain the data controllers to collect necessary data to run the system. There might be such functions that could only be available if the user shares some of the personal data. These functions should not be available to the users without obtaining their consent to process the necessary personal data. Indeed, the consent should be given in an informed basis, freely, be specific to the purpose of the specific function, unambiguous or explicit (depending on a type of personal data e.g. whether sensitive data or not), and should be given with an affirmative action (Recital 32 of the GDPR). The latter criterion is called as an opt-in which is more or less same meaning as the privacy by default. Opt-in action ensures that the necessary personal data is being collected and further data processing activity was left to be decided by the data subjects, manually. The data subject should have options to choose between giving consent or leaving processing activity out of the functions. It is most probably very significant in the example of Facebook in 2008, and Facebook in 2017. If one may remember how creating an individual Facebook profile was working like, the users were expected to share

lots of personal information including sensitive information such as their religion, political views, nationality, etc. There was no setting available for the users to choose whether they would like to display such information on their profile or not (personal data management tool). Moreover, the users were not given a choice to restrict whom they would like to display their own profile which may include their pictures, posts, videos as well as the other information that they gave away during the profile creation. Since 2014, Facebook has changed its "everything should be public" approach to" everything should be private and manageable" approach. Now, besides the default privacy settings, Facebook users can manage third party data disclosures, set the public-private post rule on the time of posting, and manage whole privacy settings in an understandable, user-friendly interface. Altogether, Facebook seems to draw its own borders of data collection, usage, and disclosure.

Creating successful privacy-friendly systems could be possible with cooperation between the stakeholders as well as their cooperation with the individuals. Principle of Visibility and Transparency advices to create personal data protection policy and procedure documents, and to share them with the related entities and individuals. In this case, providing comprehensive, understandable and clear information to the individuals about their rights (Articles 12-23) and the remedies (Articles 77-80, Article 82 of the GDPR). It is also crucial for the data controllers to inform the Data Protection Authority (DPA) about these policies because in the end, they will be monitored by the DPA whether they are in compliant with the law or not. While the compliance is an important issue, all the steps are taken toward to Respect for User Privacy. Cavoukian suggests to "keep the design user centric" by providing the necessary tools and information to the users to be able to execute their own data self-management. The GDPR strengthens many of these tools such as by interpreting the conditions for

consent clearly (Article 7), introducing consent mechanism for children (Article 8), introducing the Right to be Forgotten (Article 17), and right to data portability (Article 20). The companies offer users creative and user-friendly interfaces to access and manage their data. Google offers data management and Privacy Check platform designed with figures, animations, including short and understandable documents, and a control panel to manage all related data and information collected by Google. As much as personal data is being processed, such data control panel should be design as easy to be used by all users.

Finally, one may wonder to ask, what will happen if Data Protection by Design principles are implemented? First of all, the systems as well as the data will be secured in Lifecycle Protection which stresses the importance of the continuous and standard data security applications, and their balance between the functionality of the system and users' rights. As long as new technological developments, such as Artificial Intelligence and robots, become a part of people's daily life, there is a positive signal for ongoing changes and improvements in the data protection field both from a legal and practical point of view. For this reason, data protection is such a dynamic field which requires constant system monitoring to keep the level of protection or implementations, or to create even higher protection tools. Secondly, if the DPbD principles are followed, any actor involving the data processing activity will found themselves in a Win-Win position. In this way users could use the system without any doubt about how their data is being used, and as a result of the DPbD, the system stakeholders ensure adequate level of data security within the systems which they can reflect to the users and data protection authorities whether they are in compliance with the privacy policies, rules and legislation.

To summarize these thoughts, we argue that all parties of operating and using a Fog application related to a member State of the EU should be aware of the GDPR, and PET is an approach that could be applied in IoT/Fog/Cloud environments. The possible Fog use cases we depicted in Figure 16.1. highlight that multitenancy is even more existent in IoT and Fog environments than in purely cloud setups, and the number of participating entities is also higher (specifically in multiple Fog regions), which means that the correct identification of controller and processor roles are crucial.

16.6 Future research directions

The result of our investigation shows that the Data Protection by Design principle could reduce possible privacy harms of IoT applications in Cloud and Fog environments by combining the Data Protection Impact Assessment and the Data Protection Enhancing Technologies. In the future we plan to further analyze IoT, Fog and Cloud use cases and perform legal role mappings to reveal responsibilities and provide hints for designing and operating applications in these fields.

16.7 Summary

Following the recent technological trends, IoT environments generate unprecedented amounts of data that should be stored, processed and analyzed. Cloud and Fog technologies can be used to aid these tasks, but their application give birth to complex systems, where data management raises legal issues to comply with. The European Commission has started to modernize its legal system for the protection of personal data to respond to the use of these new technologies to strengthen users' influence on their personal data, to reduce administrative formalities, and to improve the clarity and coherence of the EU rules for personal data protection. To achieve these

goals, the Commission created a new legislative proposal, called General Data Protection Regulation, which we analyzed in this chapter in detail.

In this chapter we also introduced Fog characteristics and security challenges in the light of the new European legislation. We further detailed the data protection by design principle, and suggested the use of Privacy Enhancing Technologies to comply with the regulation and to ease the management of Fog environments.

Acknowledgement

The research leading to these results was supported by the UNKP-17-4 New National Excellence Program of the Ministry of Human Capacities of Hungary, and by the Hungarian Government and the European Regional Development Fund under the grant number GINOP-2.3.2-15-2016-00037 ("Internet of Living Things").

References

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems, 25:599-616 (2009).

[2] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelffle. Vision and Challenges for Realising the Internet of Things. CERP IoT - Cluster of European Research Projects on the Internet of Things, CN: KK-31-10-323-EN-C, March 2010.

[3] European Commission. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 9546EC (General Data Protection Regulation). Official Journal of the European Union, Last visited on June 17, 2017.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, pp. 31-50, 1995.

[5] A. V. Dastjerdi, R. Buyya, Fog Computing: Helping the Internet of Things Realize Its Potential. Computer, vol. 49, pp. 112-.116 (Aug. 2016).

[6] B. Escribano, Privacy and Security in the Internet of Things: Challenge or Opportunity. OLSWANG. Available: http://www.olswang.com/media/48315339/privacy_and_security_in_the_iot.pdf, Nov. 2014.

[7] Opinion 8/2014 on the on Recent Developments on the Internet of Things. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, Oct. 2014.

[8] S. Yi, Z. Qin, and Q. Li. Security and privacy issues of fog computing: A survey. In International Conference on Wireless Algorithms, Systems, and Applications (pp. 685-695). Springer, Cham, 2015, August.

[9] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh. On security and privacy issues of Fog computing supported Internet of Things environment. In IEEE 6th International Conference on the Network of the Future (NOF), pp. 1-3, September 2015.

[10] M. Mukherjee et al., Security and Privacy in Fog Computing: Challenges. IEEE Access, vol. 5, pp. 19293-19304 (2017).

[11] A. Kertesz, Characterizing cloud federation approaches. In: Cloud computing: challenges, limitations and R&D solutions. Computer communications and networks. Springer, Cham, pp. 277-296, 2014.

[12] R. Want, S. Dustdar, Activating the Internet of Things. Computer, Vol. 48, No. 9, pp. 16-20 (2015).

[13] L. Atzori, A. Iera, and G. Morabito, The Internet of Things: A Survey. Comput. Netw., Vol. 54, No. 15, pp. 2787-2805 (2010).

[14] A. Kertesz, Sz. Varadi, Legal Aspects of Data Protection in Cloud Federations. In S. Nepal & M. Pathan (Ed.), Security, Privacy and Trust in Cloud Systems, pp. 433-455, Berlin, Heidelberg. Springer-Verlag, 2014.

[15] A. Cavoukian, Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, 2011.

[16] I. Rubinstein, Regulating Privacy by Design. Berkeley Technol. Law J., vol.26, p.1409 (2011).

[17] E. Everson, Privacy by Design: Taking Ctrl of Big Data. Cleveland State Law Review, vol. 65. pp. 27–44 (2016).

[18] A. Rachovitsa, Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue. Int. J. Law Inf. Technol., vol. 24, no. 4, pp. 374–399 (2016).

[19] P. Schaar, Privacy by Design. Identity Inf. Soc., vol. 3, no. 2, pp. 267–274 (2010).

[20] Apple Inc. Apple's commitment to your privacy. Available: https://www.apple.com/privacy/, December 2017.

[21] Information Commissioner's Office (ICO), Conducting privacy impact assessments code of practice, 2014. Available: https://ico.org.uk/media/for-organisations/documents/1595/- pia-code-of-practice.pdf

[22] N. Hodge, The EU: Privacy by Default Analysis. In-House Perspective, vol. 8. pp. 19-22, 2012.

[23] K. A. Bamberger and D. K. Mulligan, PIA Requirements and Privacy Decision-Making in US Government Agencies. In Privacy Impact Assessment, D. Wright and P. De Hert, Eds. Dordrecht: Springer Netherlands, pp. 225-250, 2012.

[24] Privacy and Data Protection by Design – from policy to engineering, European Union Agency for Network and Information Security (ENISA), 2014.